International Journal of Pure and Applied Mathematics
Volume 119 No. 17 2018, 1451-1464
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

A Comparative Study on the Difference Between Conventional Crime and Cyber Crime

[1]G.K. Ayswariya and [2]Aswathy Rajan

[1]Saveetha School of Law,

Saveetha Institute of Medical and Technical Sciences,

Saveetha University,

Chennai.

gkaywariya15@gmail.com

[2]Saveetha School of Law,

Saveetha Institute of Medical and Technical Sciences,

Saveetha University,

Chennai

aswathyrajan.ssl@saveetha.com

Abstract

These days, an association reliance on cyberspace is turning into an inexorably part of authoritative security. The foundation of various associations are interconnected in cyberspace, consequently the level of hazard to security has expanded significantly. The risk to cyber security is developing at tremendous rate. One of the contrasts amongst cybercrime and customary crime is the confirmation of the offenses. Conventional lawbreakers as a rule leave hints of a crime, through either fingerprints or other physical confirmations. Then again, cybercriminals depend on the Internet by means of which they carry out their crimes, and it leaves next to no proof about the cyber crime. The second contrast amongst conventional and cybercrime is length of examinations. Since cybercrime includes culprits utilizing misrepresented names and working from remote areas, it more often than not takes more time to distinguish the genuine cyber hoodlums and catch them. As a rule, cyber offenders escape from capture in light of the fact that the agents can't find them. Conventional crimes take shorter day and age to examine in light of the fact that the offenders as a rule leave prove that can be utilized to spot them.

Another contrast between conventional crimes and cybercrimes is the power included. The vast majority of the conventional crimes, (for example, assault, murder, pyro-crime, and thievery among others) include the

utilization of over the top power that outcomes in physical damage and injury on the casualties. Then again, cyber crimes don't require the utilization of any power since the culprits simply utilize the characters of their casualties to take from them.

Key Words: Cyber crime, conventional, traditional, modern, comparison, hacking, data, computer.

1. Introduction

Cyber crime is not quite the same as conventional crime in different ways, yet two noteworthy contrasts are that, In cyber crimes, the culprit is regularly significantly harder to find, distinguish, and in the end get. Numerous individuals utilize the web, content informing, and online networking to take cover behind a virtual character which, basically, can be anything and anybody they need. With the new capacities we have nowadays, anybody can figure out how to utilize the web further bolstering their good fortune and thus utilize it to hurt others. Hacking, which basically was outlandish (or exceptionally unrealistic) until of late, has turned out to be shockingly simple on the off chance that somebody can get the correct data. With conventional crime, the culprit doesn't have an indistinguishable capacity from inside cyber crime. While still difficult, cyber crime is a significantly less demanding approach to get what somebody needs. Some X person via web-based networking media could be your nearby neighbor and you'd never know it. With expanding information of PCs and how to utilize and control them, cyber crimes are more probable than at any other time. Programmers from different nations are disturbing atomic power plants, individuals are having their personalities and whole lives stolen from them. Cyber crime, while entirely different from conventional crime, is as yet an appalling offense.

2. Aim of the Study

To discuss about what is a cyber crime

To know about conventional crime and its impacts

To deal with the differences between conventional crime and cyber crime

To analyse and compare the differences of conventional crime and cyber crime

To also deal with the seriousness of offences and punishments under conventional crime and cyber crime

Hypothesis

H0: There is no significant impact on cyber crime when compared to conventional crime

Ha: There is significant impact on cyber crime when compared to conventional crime

3. Materials and Method Used

A Doctrinal method of research is being done on this paper. And the research is done with the help of secondary sources such as books and e-sources.

4. Review of Literature

1. A comparative study on cyber crime in criminal law, Qianyun Wang
2. This article deals about the comparative study of what ways and methods has been used to commit cyber crime in various countries like data diddling, salami attacks, web jacking, computer system theft, physical damage, Trojan attack, demarcation etc.
3. Classification of cyber crime and its differentiation from conventional crime, Vivek Sharma
4. The fastest growing technologies has paved way for more cyber crimes. Cyber crime done against individual property and organization are dealt with. Conventional crime targets individual and they are appreciable involvement medium of sine quo non.
5. Physical and Cyber crime: A brief comparative analysis, Darin Swan, University of Maryland
6. Cyber crime differ from conventional crime in many ways like finding the wrongdoer, difficult to find in the commission in a cyber crime whereas in a conventional crime it is quite easy because cyber crime lacks proper evidence.
7. Cybercrime and traditional crime-are they interconnected? Turn the alarm back on improving good governance with e-policy management, Kevin Mitnick
8. In traditional crime we can find traces of fingerprints, blood samples, weapon used etc, but no traces are left in a cyber crime. It has been committed online and only technological experts can find the wrongdoer in a cyber crime.
9. Cyber crime vs Traditional crime, Ian Carnaghan

The complexities of catching cyber criminals meant that in the past many have gotten away with their crimes and they do not face the same punishment as traditional criminals which most likely lead the attraction of committing crime in the first place.

5. A Comparative Analysis on the Difference between Conventional Crime and Cyber Crime

One of the contrasts amongst cybercrime and conventional crime is the proof of the offenses. Customary crooks for the most part leave hints of a crime, through either fingerprints or other physical confirmations. Then again, cybercriminals depend on the Internet by means of which they carry out their crimes, and it leaves next to no proof about the cybercrime. Scientific agents normally encounter awesome trouble in get-together confirmation that could prompt the conviction of cybercriminals since these lawbreakers can uninhibitedly change their characters. The Internet additionally permits the obscurity of its clients, and this infers cybercriminals can utilize any nom de plumes their

distinguishing proof. Then again, it is troublesome for conventional hoodlums to counterfeit their sexual orientation, race, or age.

Therefore, this prompts the second contrast amongst customary and cybercrimes, length of examinations. Since cybercrime includes culprits utilizing distorted names and working from remote areas, it for the most part takes more time to recognize the genuine cybercriminals and secure them. By and large, cybercriminals, (for example, programmers) escape from capture on the grounds that the specialists can't find them. Conventional crimes take shorter day and age to explore in light of the fact that the hoodlums as a rule leave prove that can be utilized to spot them. For example, customary hoodlums can leave confirmation, for example, DNA, fingerprints, photos and recordings caught on reconnaissance cameras, or individual assets, for example, character cards, and this makes it simple for examiners to recognize and catch the guilty parties. Furthermore, such confirmation makes it simple for the legal to convict the guilty parties.

Cybercriminals can utilize the Constitution to shield themselves from arraignment. The Fifth Amendment brings up that no one can be compelled to wind up an observer against himself in any criminal case. Subsequently, cybercriminals can utilize this lawful arrangement to deny the agents any implicating proof that could prompt the indictment of the cybercriminals. This suggests even in circumstances where cybercriminals are caught, the trial procedure may take long unless the specialists accumulated evident proof about the crimes.

Comparing Abetment in Cyber Crime and Conventional Crime

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for punishment of such abetment, be punished with the punishment provided for the offence under this Act under Section 84B of Indian Penal Code.

Bailable and Non-Bailable Offences

Under the existing Information Technology Act there is no specific provision regarding the classification of cognizable, non-cognizable or bailable, non-bailable or otherwise hence the classification of cyber crime cases has to be decided in accordance with Section 2(a) and 2(c) read with 1st Schedule of the Cr.P.C in which the conventional crimes are dealt with.

Comparing the Punishments in Cyber Crime vs. Conventional Crime

The complexities in getting cyber criminals have implied that previously numerous people have become away with their crimes and don’t confront the same punishment as that of conventional offenders, which no doubt prompt the

fascination of carrying out the crime in any case. While laws have been ease back to adjust to these more up to date types of criminal movement, advance has been made. A couple of years ago, malevolent programmers could take a great amount of money, they cause mass harm but then escape imprisonment. These days prosecution have enormously risen along with imprisonment to those sentences. It is difficult to say that cyber crime should be punished the same, more or less severely than conventional offenders because there is no clear way to compare both of them. It cannot be said that all the time that cyber criminals get less serious punishments than conventional crimes because money play a very vital role in our day to day life.. Sometimes wealthy men who have committed heinous offences like rape and murder can give money to the authorities and can easily escape from the clutches of law whereas poor men who had hacked some website, data theft or any form of cyber crime has to suffer many years of imprisonment in jail. This is the exact scenario nowadays.

The Purpose of Most Hackers

The principle goal of numerous programmers is to discover shortcomings, vulnerabilities, and bugs in PC frameworks. Be that as it may, individuals may participate in hacking for various reasons, for example, hacking for no particular reason, criminal pick up, making explanations, or enhancing security. Individuals who hack for no particular reason do as such to demonstrate their specialized abilities in breaking computerized security frameworks. Such programmers are not keen on the data they access from hacking different PCs. Individuals who hack for criminal pick up do as such to swindle their casualties by getting to and controlling their own information. Such programmers utilize monetary data and passwords of the casualties to move their assets into private records, and this may bring about enormous budgetary misfortunes to the casualties.

People who hack to create an impression do as such to make ideological or political focuses by taking arranged data from business and government databases. As a rule, the programmers assault these associations to challenge inertia by the legislature in tending to different issues or shameful acts executed by private organizations. At long last, the last gathering of programmers is the people who participate in hacking to enhance the advanced security frameworks of different associations. Such people are generally utilized to recognize any vulnerabilities and bugs in the advanced security frameworks of organizations. This helps the organizations in enhancing the security of their frameworks and averts assaults by vindictive programmers.

Cybercrime for the most part has budgetary outcomes since it brings about loss of protected innovation, money related misfortune and corruption of shopper trust in different associations. Such misfortunes have extensive effects to the general public. Cybercrimes cause exchange contortions, work misfortunes, loss of intensity of influenced associations, prosecution costs in paying influenced

customers, and expanded protection costs. All these tend to reclaim the additions made in the general public.

Cybercrime is one of the cutting edge challenges that specialists are looked with today. Its regularly advancing face makes it trickier to manage. The wide degree achieved by the web likewise makes examinations concerning cybercrime substantially more requesting. Powerful cross-fringe participation is expected to definitively decide the vast majority of the cases

In spite of the fact that we discuss cybercrime as a different element to conventional crime, it is completed by similar sorts of lawbreakers for a similar kind of reasons.

These programmers are proficient hoodlums, criminal packs, displeased workers, proficient rivalry, activists, frustrated youth and state enemies. They have an indistinguishable inspirations from customary offenders, for example, weariness and vandalism, ideological or political help, malevolence or requital, fiscal increase through coercion or offer of unlawfully got information, psychological warfare or reputation and drama.

The strategies that cyber crooks use to assemble information and play out an assault is tantamount to physical 'conventional' crimes. For instance, how about we look at how a criminal pack may approach breaking into a bank to take cash against how a cyber criminal group may approach breaking into a PC system to take information.

The Scale

Assaults can be directed on a scale impractical in the physical world. A customary bank burglar may just have the capacity to hit maybe a couple banks seven days, a cyber-assault can focus on 100's if not 1000's of locales on the double.

The Reach

Assaults can be performed from anyplace on the planet; they can be performed secretly and inside locales where the outcomes of those activities may not, or can't, be tended to by the criminal equity framework. Assailants are likewise ready to separate significantly more information carefully than could ever be conceivable in the physical world. For instance 1 gigabyte of information is around 4,500 soft cover books. Consider what number of gigabytes of information is hung on a framework, programmers can extricate this inside a matter of minutes.

Perception and Media Effect

There is another piece of the cyber risk to be viewed as, general society and media impression of cyber crime. At the point when expansive money related

foundations have been hacked the media has frequently entirely allotted fault to the associations as opposed to the offenders, this would not be the situation in a physical bank theft.

6. Case Laws

Recent Incident

Over 22,000 Indian websites hacked, March 7, 2018

According to data answered to and followed by Indian Computer Emergency Response Team (CERT-In), a sum of 22,207 Indian sites including 114 government sites were hacked amid April 2017 to January 2018. An aggregate number of 493 influenced sites were utilized for malware spread," Minister of State for Electronics and IT K J Alphons said in a composed answer to Lok Sabha. Furthermore, according to the data answered to and followed by National Informatics Center (NIC), an aggregate number of 74 and six government sites facilitated on NICNET were hacked amid 2017 and 2018 (till February), separately, he included. The clergyman said 301 security cautions with respect to potential vulnerabilities and dangers to various frameworks and applications were issued by CERT-In amid April 2017-January 2018. Also, different custom fitted cautions were sent to key associations to empower them to distinguish and avoid cyber assaults. In light of a different question, Alphons said all the new government sites and applications are to be reviewed concerning cyber security before their facilitating alongside review all the time subsequent to facilitating. Associations utilize servers to have sites and applications for scattering of data and giving administrations to clients. The servers not designed appropriately and having powerless programming are inclined to hacking and could be abused by cyber lawbreakers.

He included that ceaseless endeavors are required to be made by proprietors to ensure servers by method for solidifying and sending fitting security controls. To an inquiry on whether counterfeit news had infested all circles of life and had prompted genuine repercussions, he said the administration does not keep up particular data on individuals booked in segregated episodes for course of phony news on informing and web-based social networking stages. Alphons, because of another inquiry, said so as to work towards key mediations to advance counterfeit consciousness applications, the legislature has set up four boards of trustees of specialists from the scholarly community, industry and government.
These councils will investigate zones like stages and information for Artificial Intelligence, utilizing Artificial Intelligence for distinguishing national missions in key areas, skilling and reskilling, and cybersecurity, safety, legal and moral issues.
The pastor noticed that the interest in STPI (Software Technology Parks of India) units in 2016-17 remained at Rs 14,099 crore, while that in IT units in Special Economic Zones (SEZ) was at Rs 1,36,781 crore.

Indian Debit card hacks, 20 October 2016

The break is accepted to have occurred about a month back. This all began when numerous individuals in India announced unapproved exchanges through their charge cards. These exchanges are said to have been followed to China and US. Quickly after this concise scene a huge number of individuals in India began accepting SMS from their particular banks that they have to change their ATM card PIN number. The SMS likewise educated them that their universal exchange restrict was diminished to Rs 7000. The purposes behind the same were not educated. An assessment is coming to fruition among open to consider banks responsible for breaks. Initially, there is a rising interest for a rupture divulgence law that orders the banks to uncover all insights about the breaks. India doesn't have a rupture divulgence law and in this way individuals don't come to think about the subtle elements of any breaks that have occurred in the budgetary establishments wherein they have their cash kept. In the greater part of the states in US and numerous nations in the EU break divulgence laws have been set up since decades. These laws make it obligatory for banks to self reveal all ruptures that happen at their finishes. Once the law is set up and obligations are unmistakably settled, individuals can be considered responsible.

Vladimir Levin vs. Citibank (1995)

Levin's case is among the primary prominent instances of hacking for criminal pick up. Vladimir, an individual from a Russian crime ring, prevailing with regards to hacking into Citibank's system and taking classified data of Citibank's clients. Utilizing the client passwords and codes, Vladimir exchanged roughly $3.7 million without the bank's information or assent (Goodchild, 2012). Vladimir exchanged the stolen cash to accounts partnered to his criminal association. Citibank developed suspicious that its framework had been assaulted in the wake of distinguishing two exchanges of $304,000 and $26,000. The bank educated the FBI about the issue, and the FBI figured out how to track Vladimir in London. Vladimir was captured at London's Heathrow Airport in 1995. After his catch, Citibank figured out how to recuperate a large portion of the stolen cash. In 1998, an American Court gave Vladimir a three-year sentence and requested him to restore $ 240,000 to Citibank.

Varpaul Singh v. State of Punjab (April 19, 2010)- CITATION 850482

This petition has been documented under Section 438 Cr.P.C. for concede of bail to the petitioner on the off chance that FIR No. 328 dated 16.12.2009 under Sections 420, 406, 120-B IPC read with Section 65 of the Information and Technology Act, 2000 enrolled with Police Station, Sadar, Jalandhar. Learned Counsel for the petitioner battles that the petitioner was working in supervisory limit and had nothing to do with money gathered. It was the Cashier's activity and along these lines, the petitioner couldn't have been embroiled. It has additionally been contended that the petitioner had made a request against the complainant, M/s Makkar Motor Private Limited, Jalandhar for raising

compensation. It is in counter impact to the said request that the petitioner has been erroneously involved. Learned Counsel additionally expresses that every one of the records have been surrendered by the petitioner and he isn't required for facilitate examination. It has been fought that the Managing Director of the Company needed the petitioner to sign certain claim/protection papers to empower the Company to get a claim against the harm to his property. The petitioner did not sign the archives and consequently has been ensnared for the situation. I have thought about the disputes of learned Counsel. According to the FIR, petitioner was working in the limit of General Manager of M/s Makkar Motor Private Limited. In encouragement of the basic goal of the charged, imaginary bills and sections were made. Imperative information was erased from the PCs. Related records were taken away by method for conferring the offense of robbery. Save parts had been sold/stolen. Significant sum has been stashed by the denounced said in the FIR. The way in which the offense has been submitted, has been given in detail in the FIR which demonstrates that supposedly the petitioner, under whose supervision the work was being done in the workshop, enjoyed getting ready false bills. Charge is likewise such that he abused the certainty rested in him by method for giving him access to the fundamental edge. The secret word depended for a specific intention was utilized to change the information in the PC framework. Assertion is likewise such that while more cash was charged, the imperfections in the vehicles were not corrected. Bills for the work done were erased from the PC principle outline. Points of interest of the way in which the offense has been conferred, isn't required to be given while managing this petition under Section 438 Cr.P.C. Do the trick it to state that unwinding the way in which the wrongdoing purportedly has been conferred, would require custodial cross examination. Affirmation is of expulsion of record as likewise erasure of material from the PC fundamental edge. Learned Counsel for the respondent-State has called attention to that the petitioner has taken away material record which is required to be recouped. Without custodial cross examination of the petitioner, the researching organization would not be in a situation to arrive at a legitimate conclusion. I have considered the affirmations made in the FIR against the petitioner with regards to contentions tended to by the learned Counsel.

It isn't in debate that the petitioner had been functioning as General Manager. In such conditions, it can't be said at this phase the petitioner had nothing to do with the money or supervision of repair of vehicles and arrangement of bills. So far as the conflict of learned Counsel for the petitioner such that petitioner has been dishonestly ensnared on the grounds that he had raised an interest for raising pay and in light of the fact that he had declined to sign the claim/protection papers to empower the Managing Director to get a claim, is concerned, definitely the examining organization would investigate that perspective moreover. Considering the way in which the offense has been submitted, I am of the view that verified actualities can be separated just through custodial cross examination. In perspective of the over, no ground for bail under Section 438 Cr.P.C. is made out. The petition is dismissed.

Regina v. Graham Waddon ,1999, Appeal Cases [2007] 2 A.C. 262 All England Law Reports [2007] 3 All. E.R. 757 All England Law Reports (European Cases) [2007]

Facts
The Appellant ran a business called Global Web Suites which designed the sites for MJES Group. The police accessed one such site, known as extreme-perversion. A police constable subscribed to this web-site using a pseudonym and, a couple of days later, received a password via e-mail. He printed various pornographic images from his desktop computer at the station.

The Appellant was arrested and charged with publishing obscene articles contrary to Section 2(1) of the Obscene Publications Act 1959. On 30 June 1999 he pleaded guilty at Southwark Crown Court following a ruling made by His Honour Judge Hardy rejecting two submissions on behalf of the Appellant as to legal matters. The appeal concerned the first submission, by which the Appellant claimed that the Southwark Crown Court did not have jurisdiction to try the case as there was no publication for the purposes of the Obscene Publication Act 1959 in England: the website was based in the United States.

Judgment
Rose LJ rejected the accommodation. Segment 1(3) of the Obscene Publications Act 1959 gives:

For the reasons for this Act a man publishes an article who – (b) on account of an article containing or encapsulating matter to be taken a gander at or a record, appears, plays or extends it, or, where the issues is information put away electronically, transmits that information.

The Appellant surrendered that he, or through his operators, was included both in the transmission of material to the site in the United States and its transmission back to England and subsequently he couldn't battle that production did not happen in this nation. The Court of Appeal held that it was not the case that there must be single distribution yet that various productions could happen. There might be production on a site abroad when pictures are transferred and there can be further distribution when the pictures are downloaded somewhere else. The Court declined to guess on the outcome where obscene material was transferred to an area out of the ward planning that there ought to be no transmission of that material back to the UK. That would require thought of inquiries of aim and causation in connection to where the production should happen.

7. Conventions, Agreements and Treaties

Budapest Convention on Cybercrime and The Convention on the Prevention and Punishment of the crime of Genocide are the two conventions related to the paper. India is a party to The Convention on the Prevention and Punishment of

the crime of Genocide and unfortunately India is not a party to the Budapest Convention on Cyber Crime, it is yet to become a party of it.

8. Suggestions

Severe punishments should been given for cyber crime like conventional crimes. Speedy trial should be there in cyber crimes so that we can avoid suicidal tendencies of cyber crime. The punishments applicable for abetting someone to commit suicide in a conventional crime should be the same also for abetment to commit suicide or suicidal tendencies occurred as a result of any cybercrime.

9. Conclusion

In conclusion, the distinction between conventional crimes and cybercrimes is the power included. The greater part of the customary crimes, for example, assault, murder, incendiarism, and thievery among others include the utilization of unnecessary power that outcomes in physical damage and injury on the casualties. Then again, cybercrimes don't require the utilization of any power since the offenders only utilize the personalities of their casualties to take from them. For instance, cybercriminals utilize mocking and phishing to acquire individual data, for example, credit card numbers from their casualties, or utilize scrambled messages to organize viciousness remotely. Hence there is significant impact on cyber crime when compared with conventional crime.

References

[1] A Comparative study of Cyber crime in criminal law. Qianyun Wang

[2] Classification of cybercrime and its differentiation from conventional crime, Vivek Sharma

[3] Physical and Cyber crime: A brief comparative analysis, Darin Swan, University of Maryland

[4] Cyber crime and traditional crime-are they interconnected? Turn on the alarm back on improving good governance with e-policy management, Kevin Mitnick

[5] Cybercrime v. Traditional crime, Ian Carnaghan

[6] Cybercrime classification and characteristics, Hamid Jahankhani A typology of cyber criminal networks from lowtech all rounders to high-tech specialists, E-Rutger Leukfeldt, Wouter P. Stol

[7] Ms.Rohini Arora v. Government of Net of Delhi on 13 July,2012

[8] Kola Venkat Krishna Mohan online gambling case, 4 December 1999

[9] How is cyber crime different from conventional crime, Christine Reider

[10] SMC Pneumatics(India) Pvt. Ltd v. Jogesh Kwatra, suit no. 1279/2001, Delhi HC

[11] First cyber sex crime in Delhi, Ritu Kohli case, 18 July,2000

[12] Cyber crime: The evolution of traditional crime, Ruj Samani Pandora

[13] CBI arrests Pune man who hacked over 900 accounts for a fee, Press Trust of India, January 24,2014

[14] How Digital is traditional crime, intelligence and security informatics conference(EISIC),2013, 12-14 August 2013

[15] Comprehensive study on cyber crime, United Nations Office on drugs and crime, Vienna, February 2013

[16] Cyber crime: A review of the evidence , Mike Mc Guire, University of Surrey and Saamantha Dowing, Home Office Science, October 2013

[17] Introduction to cyber crime, William Gibson

[18] Relation between conventional crime and cyber crime, Legal Point Foundation

[19] Pranab Kumar v. State of West Bengal, 26 August,2013